

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended) A method to facilitate secure messaging,
2 comprising:
3 creating a message at an origin;
4 computing a digest of the message;
5 signing the digest using an origin private encryption key;
6 sending the message and the digest to a queue located in a third party
7 device for delivery to a recipient;
8 receiving the message and the digest at the queue;
9 verifying that the digest was signed at the origin by using an origin public
10 encryption key, whereby the origin cannot deny creating the message; ~~and~~
11 if the digest is verified as being signed at the origin,
12 placing the message and digest on the queue and persistently
13 storing a record of this transaction, and
14 notifying the recipient that the message is available;
15 generating a request at the recipient to receive the message from
16 the queue located in the third party device;-
17 creating a signature for the request using a recipient private encryption
18 key;
19 sending the request and the signature to the queue;
20 validating the request at the queue using the signature and a recipient
21 public encryption key; and

22 if the request is valid,
23 dequeueing the message from the queue,
24 sending the digest to the recipient;
25 signing the digest at the recipient using the recipient private
26 encryption key creating a signed digest;
27 returning the signed digest to the queue,
28 validating the signed digest at the queue using the recipient
29 public encryption key, whereby the recipient cannot deny
30 requesting to receive the message, and
31 if the signed digest is valid, persistently storing a record of
32 this transaction and sending the message to the recipient.

1 2. (Canceled)

1 3. (Currently amended) The method ~~of claim 2~~ of claim 1, further
2 comprising passing the message and the digest through a plurality of queues
3 between the origin and the recipient, whereby the recipient and the origin are
4 subscribers of different queues.

1 4. (Original) The method of claim 3, further comprising passing the
2 message and the digest through a plurality of databases, wherein each database in
3 the plurality of databases includes at least one queue of the plurality of queues.

1 5. (Currently amended) The method ~~of claim 2~~ of claim 1, wherein
2 the origin public encryption key and the origin private encryption key are a key
3 pair of a public key encryption system.

1 6. (Currently amended) The method ~~of claim 2~~ of claim 1, wherein
2 the recipient public encryption key and the recipient private encryption key are a
3 key pair of a public key encryption system.

1 7. (Currently amended) The method ~~of claim 2~~ of claim 1, wherein
2 computing the digest includes using one of message digest 2 (MD2), message
3 digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and
4 secure hash algorithm 1 (SHA1).

1 8. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method to facilitate secure messaging, the method comprising:

4 creating a message at an origin;
5 computing a digest of the message;
6 signing the digest using an origin private encryption key;
7 sending the message and the digest to a queue located in a third party
8 device for delivery to a recipient;
9 receiving the message and the digest at the queue;
10 verifying that the digest was signed at the origin by using an origin public
11 encryption key, whereby the origin cannot deny creating the message; ~~and~~
12 if the digest is verified as being signed at the origin,
13 placing the message and digest on the queue and persistently
14 storing a record of this transaction, and
15 notifying the recipient that the message is available;:
16 generating a request at the recipient to receive the message from the queue
17 located in the third party device;
18 creating a signature for the request using a recipient private encryption
19 key;

20 sending the request and the signature to the queue;
21 validating the request at the queue using the signature and a recipient
22 public encryption key; and
23 if the request is valid,
24 dequeueing the message from the queue,
25 sending the digest to the recipient,
26 signing the digest at the recipient using the recipient private
27 encryption key creating a signed digest,
28 returning the signed digest to the queue,
29 validating the signed digest at the queue using the recipient
30 public encryption key, whereby the recipient cannot deny
31 requesting to receive the message, and
32 if the signed digest is valid, persistently storing a record of this transaction and
33 sending the message to the recipient.

1 9. (Canceled)

1 10. (Currently amended) The computer-readable storage medium of
2 ~~claim 9~~ of claim 8, the method further comprising passing the message and the
3 digest through a plurality of queues between the origin and the recipient, whereby
4 the recipient and the origin are subscribers of different queues.

1 11. (Original) The computer-readable storage medium of claim 10, the
2 method further comprising passing the message and the digest through a plurality
3 of databases, wherein each database in the plurality of databases includes at least
4 one queue of the plurality of queues.

1 12. (Currently amended) The computer-readable storage medium of
2 ~~claim 9 of claim 8~~, wherein the origin public encryption key and the origin private
3 encryption key are a key pair of a public key encryption system.

1 13. (Currently amended) The computer-readable storage medium of
2 ~~claim 9 of claim 8~~, wherein the recipient public encryption key and the recipient
3 private encryption key are a key pair of a public key encryption system.

1 14. (Currently amended) The computer-readable storage medium of
2 ~~claim 9 of claim 8~~, wherein computing the digest includes using one of message
3 digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash
4 algorithm (SHA), and secure hash algorithm 1 (SHA1).

1 15. (Currently amended) An apparatus to facilitate secure messaging,
2 comprising:

3 a first creating mechanism that is configured to create a message at an
4 origin;

5 a computing mechanism that is configured to compute a digest of the
6 message;

7 a first signing mechanism that is configured to sign the digest using an
8 origin private encryption key;

9 a first sending mechanism that is configured to send the message and the
10 digest to a queue located in a third party device for delivery to a recipient;

11 a receiving mechanism that is configured to receive the message and the
12 digest at the queue;

13 a verifying mechanism that is configured to verify that the digest was
14 signed at the origin by using an origin public encryption key, whereby the origin
15 cannot deny creating the message;

16 a placing mechanism that is configured to place the message and digest on
17 the queue and persistently store a record of this transaction; and
18 a notifying mechanism that is configured to notify the recipient that the
19 message is available;
20 a generating mechanism that is configured to generate a request at the
21 recipient to receive the message from the queue located in the third party device;
22 a second creating mechanism that is configured to create a signature for
23 the request using a recipient private encryption key;
24 a second sending mechanism that is configured to send the request and the
25 signature to the queue;
26 a first validating mechanism that is configured to validate the request at
27 the queue using the signature and a recipient public encryption key;
28 a dequeueing mechanism that is configured to dequeue the message from
29 the queue;
30 a third sending mechanism that is configured to send the digest to the
31 recipient;
32 a second signing mechanism that is configured to sign the digest at the
33 recipient using the recipient private encryption key creating a signed digest;
34 a returning mechanism that is configured to return the signed digest to the
35 queue;
36 a second validating mechanism that is configured to validate the signed
37 digest at the queue using the recipient public encryption key and persistently store
38 a record of this transaction, whereby the recipient cannot deny requesting to
39 receive the message; and
40 wherein the third sending mechanism is further configured to send the
41 message to the recipient.

1 16. (Canceled)

1 | 17. (Currently amended) The apparatus ~~of claim 16~~ of claim 15, further
2 comprising a passing mechanism that is configured to pass the message and the
3 digest through a plurality of queues between the origin and the recipient, whereby
4 the recipient and the origin are subscribers of different queues.

1 | 18. (Original) The apparatus of claim 17, wherein the passing
2 mechanism is further configured to pass the message and the digest through a
3 plurality of databases, wherein each database in the plurality of databases includes
4 at least one queue of the plurality of queues.

1 | 19. (Currently amended) The apparatus ~~of claim 16~~ of claim 15,
2 wherein the origin public encryption key and the origin private encryption key are
3 a key pair of a public key encryption system.

1 | 20. (Currently amended) The apparatus ~~of claim 16~~ of claim 15,
2 wherein the recipient public encryption key and the recipient private encryption
3 key are a key pair of a public key encryption system.

1 | 21. (Currently amended) The apparatus ~~of claim 16~~ of claim 15,
2 wherein computing the digest includes using one of message digest 2 (MD2),
3 message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA),
4 and secure hash algorithm 1 (SHA1).